

REMARKS

The indication of allowable subject matter in claims 3-5 is acknowledged and appreciated. In response to the pending Office Action, claims 1-10 have been amended and claim 11 has been added. Support for the present amendments and added claim may be found in the application at, for example, page 30, line 29 to page 39, line 17 and FIGS. 5-8. No new matter has been introduced.

For the reasons set forth below, Applicants respectfully submit that all pending claims as currently amended are patentable over the cited prior art.

Specification

The title of the application was objected to for allegedly not being descriptive. Applicants have amended the title to overcome this objection.

Claim Objections

Claim 9 was objected to due to a typographical error. Applicants have amended claim 9 to overcome this objection.

Claim Rejections – 35 U.S.C. § 112

Claims 3 and 4 were rejected under 35 U.S.C. § 112, first paragraph. Applicants have amended claims 3 and 4 to overcome the § 112, first paragraph rejection.

Claims 1-10 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. Applicants have amended claims 1-10 to overcome the § 112, second paragraph objection.

Claim Rejections – 35 U.S.C. § 102

Claim 1 was rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Number 5,237,616 (“Abraham”). Applicants respectfully traverse the § 102(b) rejection for at least the following reasons.

Claim 1 recites an information processing apparatus for accessing memory spaces including a user memory space and a secure memory space. The information processing apparatus includes a general purpose register, a secure information unit, a data control unit, and an address control unit. The general purpose register is used for an arithmetic operation of a CPU and has a function of receiving, delivering and storing data. The general purpose register includes a data unit.

The secure information unit is included in the general purpose register and is adapted to be set to a state not requiring security in a case that the data is transferred from the user memory space to the data unit of the general purpose register and is adapted to be set to a state requiring security in a case that the data is transferred from the secure memory space to the data unit of the general purpose register. The data control unit has a function of determining whether a value of the secure information unit is in the state requiring security or the state not requiring security when the data of the general purpose register is written in the user memory space, thereby determining whether a data transfer to the user memory space is prohibited or not.

As noted above, the information processing apparatus also includes the address control unit. The address control unit has a function of determining which of the user memory space and

the secure memory space is indicated by an address information, and selecting the value of the secure information unit.

To provide context for subject matter of claim 1, a non-limiting example in the specification describes on page 3, lines 14-29 that

In the case where the data are stored in a general purpose register by the CPU operation, the address control unit checks which memory space the data is associated with. In the case where the data is read from the user memory space, the address control unit sets the secure information unit to the state requiring no security. In the case where the data are read from the secure memory space, on the other hand, the secure information unit is set to the state requiring security. When transferring the data of the general purpose register to the user memory space, the data control unit checks the secure information unit, and in the case where the state requiring no security prevails, the data transfer is allowed. In the case where the state requiring security prevails, on the other had, the data transfer is prohibited.

Applicants respectfully request reconsideration and withdrawal of the rejection of claim 1 and its dependent claims because Abraham fails to describe or suggest an information processing apparatus that includes, among other features, a secure information unit included in the general purpose register and adapted to be set to a state not requiring security in a case that the data is transferred from the user memory space to the data unit of the general purpose register, and adapted to be set to a state requiring security in a case that the data is transferred from the secure memory space to the data unit of the general purpose register and a data control unit having a function of determining whether a value of the secure information unit is in the state requiring security or the state not requiring security when the data of the general purpose register is written in the user memory space, thereby determining whether a data transfer to the user memory space is prohibited or not, as recited in claim 1.

Abraham relates to an apparatus and method for permitting a computer to be operated in either a privileged state or an unprivileged state. Abraham at Abstract. In the privileged state, the microprocessor works with the privileged memory (105) and no data or addresses of the memory are accessible outside the secure module represented by boundary (101) in FIG. 1.

Abraham at col. 2, lines 61-65. In the unprivileged state, the microprocessor works only with memory (109) and data, addresses, and programs in the privileged memory (105) is made unavailable. Abraham at col. 2, lines 65-67.

As such, Abraham describes a system that user accessible areas (e.g., memory (105) and memory (109)) are assigned depending on CPU modes (e.g., privileged mode vs. unprivileged mode or normal mode). In contrast, in the subject matter of claim 1 the secure information unit included in the general register determines data transfer areas. Accordingly, the subject matter of claim 1 provides a different mean for determining areas where data should be transferred.

The distinction is an important one as recognized by the inventors. The inventors describe in the application that in recent development of software using open-source operating systems such as Linux, privileged mode of an OS can easily be abused to read out data in a security space and steal encryption keys and security instructions. Application at page 3, line 30 to page 4, line 5. The subject matter of claim 1 solves this problem and therefore provides an advantage over Abraham.

For at least the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 1 along with its dependent claims.

Claim Rejections – 35 U.S.C. § 103

Claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Abraham in view of U.S. Patent Number 6,101,586 (“Ishimoto”) and in further view of U.S. Patent Number 5,414,864 (“Koizumi”). Claims 7-8 and 10 were rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, U.S. Patent Number 5,680,581 (“Banno”), and U.S. Patent Number 5,386,552 (“Garney”). Claim 9 was rejected under § 103(a) as being unpatentable over

Abraham, Ishimoto, Koizumi and Banno. Applicants respectfully traverse § 103(a) rejections. The following remarks first address the rejection of claim 6, then address the rejection of claim 9, and finally addresses the rejections of claims, 7, 8, and 10.

Claim 6 recites an information processing apparatus for accessing a user memory space and a secure memory space. The information processing apparatus includes, among other features, a secure information generating unit for determining which of the user memory space and the secure memory space is indicated by address information, and delivering data with secure information into a general purpose register with secure information having a function of receiving and holding the data with secure information and a built-in RAM space for receiving and holding the data with secure information from the general purpose register and delivering the data with secure information held to the general purpose register.

Applicants respectfully request reconsideration and withdrawal of the rejection of claim 6 because Abraham, Ishimoto, and Koizumi, either alone or in combination, fail to describe or suggest an information processing apparatus that includes (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the secured information to the general purpose register having the function of holding the data with the secure information, (2) a built-in RAM space for receiving and holding the data with secure information from the general purpose register, and (3) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the general purpose register, as recited in claim 6.

As noted above, in Abraham, user accessible areas are determined based on the privileged mode or the unprivileged mode of the CPU. The privileged mode or the unprivileged

mode of the system are determined by addresses. Abraham at col. 3, lines 5-31. However, nowhere does Abraham describes or suggest assigning to the data itself a particular mode and storing the data with the particular mode.

Accordingly, Abraham fails to describe or suggest an information processing apparatus that includes an information processing apparatus including (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the secured information to the general purpose register having the function of holding the data with the secure information, (2) a built-in RAM space for receiving and holding the data with secure information from the general purpose register, and (3) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the general purpose register, as recited in claim 6.

The distinction is important as noted above. In particular, in the subject matter of claim 6 data protection does not depend on CPU's mode. And because of this feature, data confidentiality can be protected even if privileged mode of CPU is abused. Furthermore, as the subject matter of claim 6 allows both secure data and non-secure data to be stored in a built-in memory space, efficient use of the built-in memory space is possible.

Ishimoto and Koizumi also fail to describe or suggest the above-recited feature. Ishimoto relates to a memory access control circuit for inhibiting fraudulent access by detecting an access to a region to be protected on a memory. Ishimoto at col. 12, lines 36-39. The memory access control circuit includes address of data region in the memory that must be protected. Ishimoto at col. 12, lines 43-44. And, if the instructions seek to access this data region, the memory access

control checks to determine whether the location of the instruction is within a region in the memory that allows access to the protected region. Ishimoto at col. 12, lines 45-67.

As such, Ishimoto describes a memory access control that provides protection depending on areas where the data is allocated. That is access to the secured memory is only possible by instructions stored in a particular area in the memory. In contrast and as described below in more detail, the protection mechanism of claim 6, does not limit access based on areas. Rather, the secure information associated with the data limits the output of the respective data to an external space.

The protection mechanism of claim 6 is via associating secure information to the data read from a secure memory space. This secure information controls (e.g., prohibits) data output. With this constitution, for example, application data to be protected can be accessed with outsider's program (e.g., instructions) and be output from audio/image output devices, while digital data itself is prevented from being output. This means the subject matter of claim 6 can process protected data with a user program and can still maintain data confidentiality regardless of the location of the user program. This is one of the important features of claim 6.

Koizumi also fails to describe or suggest the above-recited features. The purpose of Koizumi's invention is to save/store registers using flags that indicate whether or not the register set is being used. Koizumi at col. 2, lines 31-42. These protective flag are not added to data but to the register set upon instructions to start/stop use of registers.

To this end, Koizumi is not seen to have any association with security. Accordingly, Koizumi also fails to describe or suggest an information processing apparatus including, among other features, (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the

secured information to the general purpose register having the function of holding the data with the secure information, (2) a built-in RAM space for receiving and holding the data with secure information from the general purpose register, and (3) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the general purpose register, as recited in claim 6.

For the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 6.

Claim 9 was rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi and Banno. Applicants respectfully traverse this rejection.

Claim 9 recites an information processing apparatus including, among other features, (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the secured information to a direct memory access unit (“DMA”), (2) a built-in RAM space for receiving and holding the data with secure information from the DMA, and (3) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the DMA.

Banno fails to remedy the shortcomings of Abraham, Ishimoto, and Koizumi to describe or suggest the above-recited features. Banno describes protecting data read from CPU. Similar to Ishimoto, Banno data protection/non protection is also executed depending on areas where data is located. *See* Banno at col. 3, lines 44-61. As such, Banno also fails to describe or suggest adding secure information to data itself to limit output of respective data with no limitation of access depending on areas (spaces).

For at least this reason, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 9.

Claims 7, 8, and 10 were rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, Banno, and U.S. Patent Number 5,386,552 (“Garney”). Applicants respectfully traverse this rejection for the following reasons.

Claim 7 recites an information processing apparatus that includes, among other features, (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the secured information to the general purpose register having the function of holding the data with the secure information, (2) a built-in RAM space for receiving and holding the data with secure information from the general purpose register, (3) an interrupt saved information unit with secure information having a function of adding, upon generation of an interrupt process, the secure information of the instruction decoder to data saved in a stack area of the built-in RAM space, and (4) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the general purpose register.

Applicants respectfully submit that Garney fails to remedy shortcomings of Abraham, Ishimoto, and Koizumi to describe or suggest the above-recited features. Garney is intended for efficient preservation of CPU’s processing state in a computer system with volatile memories and registers. Garney is not seen to describe or suggest anything about securing data, much less describing adding secure information to the data saved in a stack area of the built-in memory of the built-in RAM to thereby protect the data transfer to external space, as recited in claim 7.

For at least this reason, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 7.

Claim 8 recites features similar to the above-recited features of claim 7. Therefore, for at least the reasons presented above with respect to claim 7, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 8.

Claim 10 recites an information processing apparatus that includes, among other features, (1) a secure information generating unit that associates secure information to data read from the user memory space and the secure memory space and delivers the data with the secured information to the general purpose register having the function of holding the data with the secure information, (2) an operating unit with secure information having a function of reflecting the secure information of the instruction decoder in an arithmetic operation executed in accordance with the instruction decoded by the instruction decoder, and (3) a data output control unit having a function of determining whether the data transfer to the external space is prohibited or not by a value of the secure information set in the operating unit.

As noted above some of the features of claim 10 are similar to the features of claim 7. Furthermore, claim 10 includes feature of attaching secure information to data transferred through the arithmetic operating unit in the CPU. This feature, which is not seen in any of the cited prior art, allows for arithmetic operation using protected data while maintaining data confidentially.

For at least this reason and the reasons presented above with respect to claim 7, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 10.

Dependent Claims

Under Federal Circuit guidelines, a dependent claim is nonobvious if the independent claim upon which it depends is allowable because all the limitations of the independent claim are contained in the dependent claims, *Hartness International Inc. v. Simplimatic Engineering Co.*, 819 F.2d at 1100, 1108 (Fed. Cir. 1987). Because claims 1 and 6-10 are allowable for the reasons set forth above, it is respectfully submitted that all claims dependent thereon are also allowable. In addition, it is respectfully submitted that the dependent claims are allowable based on their own merits by adding novel and non-obvious features to the combination.

Based on the foregoing, it is respectfully submitted that all pending claims are patentable over the cited prior art. Accordingly, it is respectfully requested that the rejection under 35 U.S.C. § 103 be withdrawn.

Conclusion

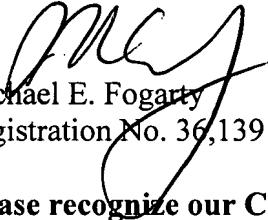
Having fully responded to all matters raised in the Office Action, Applicants submit that all claims are in condition for allowance, an indication for which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' attorney at the telephone number shown below.

Application No.: 10/764,513

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.

Washington, DC 20005-3096

Phone: 202.756.8000 MEF:MaM

Facsimile: 202.756.8087

Date: October 3, 2007

**Please recognize our Customer No. 53080
as our correspondence address.**